**IT Staff Security Policy**

All IT staff are required to understand, follow, and practice the policies and procedures that are outlined in the Employee Information Systems Security policy. These are in place to protect the computer and network infrastructure of the Library.

All IT staff will be required to sign the Employee Information Systems Security Policy agreement that all library staff are required to sign. In addition, they must agree to the following and sign the attached IT Staff Security Policy acknowledgement form.

This agreement will outline further confidentiality and security procedures and policies that **all** IT staff must adhere to.

**Authentication Credentials/Passwords**

All passwords on servers, routers, firewalls, databases, and personal Internet account passwords must be changed at least every 180 days.

These logins will be shared with all necessary IT staff so that problems may be resolved without a call to the regular operator of the equipment or software. These logins are not to be printed at any time.

Passwords will be changed immediately after any server access, maintenance, or repair by a non-library IT employee.

Failure to secure authentication credentials or passwords will result in disciplinary action according to [library’s name] policies.

**Confidentiality, Ethics, and Integrity**

We will at times work with personal files, email, financial information, and personnel files. These are confidential files and are not to be discussed or their contents disclosed outside of the necessary discussion to solve a problem or assist staff or customers that require assistance. Any misuse or sharing of confidential information will result in disciplinary action according to [library name] policies.

All library customer records are to be kept confidential according to all [library name] policies. If you are unsure of what information you may provide, contact your Supervisor or the Library Director.

**Work Ethic**

A strong work ethic will be required to maintain high levels of quality in the work performed. The IT Staff are placed in a position of such significant impact upon the business of the Library that the required level of trust can only be maintained by outstanding performance and moral conduct. Time management and punctuality are also very important to providing the best service possible to our internal and external customers. This includes: responding to email or phone messages in a timely manner, the timely completion of projects, and showing up to meetings and work on time.

**Enforcement of the Employee Information Systems Security Policy**

It is the responsibility of each IT staff person to enforce the Employee Information Systems Security Policy. Any violation of the agreement must be immediately reported to the IT Manager or the Assistant Director for Operations for any necessary actions. Failure to notify the IT Manager or the Assistant Director for Operations of an agreement violation will result in disciplinary action according to [library name] policies.

**Procedures for** **Enforcement of the Employee Information Systems Security Policy**

IT staff who discover or who are privy to information of an incident which appears to breach the Employee Security Disclosure Agreement, will follow these steps:

1. Record all relevant details and any follow-up actions. Promptly inform the IT Manager or the Assistant Director for Operations of any incidents which clearly compromise system or network integrity, including but not limited to, data loss or theft, inappropriate systems or information access, notification from outside individuals or institutions of any incident, and any other breach or violation of IT policies of which you become aware.
2. Remove the affected computer device, if appropriate, from the network and notify the IT Manager or the Assistant Director for Operations.
3. In cases where disciplinary action is not required as determined by the Human Resources Department, notify the computer/account user of the incident and request an explanation in person, by e-mail, or phone. If repeated attempts to contact the account owner fail to resolve the issues, the account may be locked.
4. In cases where disciplinary action is required, the Human Resources Department will be notified by the IT Manager or the Assistant Director for Operations to recommend the appropriate course of action before any action is taken.

**Record Keeping/Incident Logs**

IT Staff are obligated to keep all appropriate records. The following is a brief (not-comprehensive) list of records that should be kept for future use:

Server changes

Software configuration changes

Backup records

Firewall changes

Router changes

Employee Information Systems Security Policy Violations

Security breaches

Customer interactions that may require future assistance

Staff interactions that may require future assistance

Network interruptions

Each incident, maintenance, or repair report should include: date, time, a detailed narrative of the incident, step-by-step action taken (where appropriate), and date completed or closed.

**Enforcement**

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Acknowledgment of IT Staff Security Policy

This form is used to acknowledge receipt and understanding of the [library name] IT Staff Security Policy.

# Procedure

Complete the following steps:

1. Read the IT Staff Security Policy
2. Sign and date in the spaces provided below
3. Return this page only to the Human Resources Department

# Signature

By signing below, I agree to abide by the terms as outlined in the IT Staff Policy:

Employee signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee name:

Date:

Location/Branch: